

Mise en place d'une connexion SSH via clé RSA

▣ Prérequis

- Un serveur **Apache Guacamole** opérationnel
- Une machine cible avec un serveur SSH actif
- Une **clé RSA** (privée + publique)
- Un utilisateur SSH valide sur la machine cible

▣ 1. Génération d'une clé RSA

Sur la machine qui initie la connexion (par ex. Guacamole) :

```
ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/guac_key
```

▣ Option `-m PEM` nécessaire : Guacamole n'accepte pas le format OpenSSH.

- `guac_key` : clé **privée** (à coller dans Guacamole)
- `guac_key.pub` : clé **publique** (à mettre sur la machine cible)
- **Ne mettez pas de passphrase** pour éviter des problèmes

▣ 2. Déploiement de la clé publique

Sur le serveur (où se trouve sshd) :

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh

cat guac_key.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

⚙ 3. Ajustement du serveur SSH (si nécessaire)

Certaines distros récentes désactivent `ssh-rsa` par défaut.

Modifier `/etc/ssh/sshd_config` et ajouter :

```
PubkeyAcceptedAlgorithms +ssh-rsa
```

```
HostKeyAlgorithms +ssh-rsa
```

Puis redémarrer le service SSH :

```
sudo systemctl restart sshd
```

4. Configuration dans l'interface Guacamole

1. Aller dans **Connexions** → **Nouvelle connexion**
2. Choisir le **protocole SSH**
3. Remplir les champs suivants :
 - **Nom d'hôte** : IP ou domaine de la cible
 - **Port** : généralement 22
 - **Nom d'utilisateur** : ex. root
 - **Clé privée** : coller le contenu du fichier guac_key
 - **Phrase de passe** : laisser vide (si clé sans mot de passe)

5. Tester la connexion

Cliquez sur la connexion SSH : si tout est bien configuré, le terminal s'ouvre depuis le navigateur.

Dépannage : "Public key authentication failed"

Si l'erreur suivante apparaît dans les logs guacd :

```
Public key authentication failed: Username/PublicKey combination invalid
```

Vérifications à faire :

- Clé privée au format **PEM**
- Clé publique bien dans ~/.ssh/authorized_keys
- Fichier sshd_config contient :

```
PubkeyAcceptedAlgorithms +ssh-rsa
```

```
HostKeyAlgorithms +ssh-rsa
```

- Permissions correctes :
 - ~/.ssh → 700
 - ~/.ssh/authorized_keys → 600

Astuce

Pour suivre les logs en direct :

```
journalctl -u guacd -f
```

Source : [📄 Documentation Guacamole](#) [📄 Manuel OpenSSH](#)

Revision #2

Created 9 April 2025 09:04:22 by Maxime

Updated 9 April 2025 13:49:35 by Maxime